Enhancing security of DICOM images during storage and transmission in distributed environment

A LAVANYA* and V NATARAJAN

Department of Instrumentation Engineering, Madras Institute of Technology,
Chennai 600 044, India
e-mail: lavanyaananthan@gmail.com

MS received 3 September 2010; revised 5 January 2011; accepted 12 May 2011

Abstract. Digital watermarking is proposed as a method to enhance medical data security. Medical image watermarking requires extreme care when embedding additional information within medical images, because the additional information should not degrade medical image quality. Doctors diagnose medical images by seeing Region of Interest (ROI). A ROI of a medical image is an area including important information and must be stored without any distortion. If a medical image is illegally obtained or if its content is changed, it may lead to wrong diagnosis. In our scheme a well-known technique least significant bit substitution (LSB) is adapted to fulfill the requirements of data hiding and authentication in medical images. The scheme divide Digital Imaging and Communications in Medicine (DICOM) image into two parts ROI and non-ROI (non-region of interest). The DS (Digital Signature) which include patient data and SOP Instance UID are embedded randomly into the LSB border of the image. The DWT (Discrete Wavelet Transform) of ROI-MSB (most significant bit) embedded into the LSB middle of the image. The Result shows the ability to hide and retrieve DS in non-ROI, while ROI, the most important area for diagnosis, is retrieved exactly at the receiver side.

Keywords. Watermarking; ROI; LSB; DS; non-ROI; DWT; DICOM (digital imaging and communications in medicine).

1. Introduction

In recent years due to advancement of technology usage of cell phone becomes most common. The paper published in the International Journal of Epidemiology, states that there is a risk of brain tumours from cell phone use (<http://ahmedamiruddin.wordpress.com/2010/05/17/study-cellphone-brain-cancer-link/>). Brain Tumour is the most common cause of death in United States (<http://www.everydayhealth.com/brain-tumor/brain-tumor-statistics.aspx>). The treatment of brain tumours usually begins with surgery, so the doctors required ROI to diagnose brain

*For correspondence

tumour. Brain tumour Image is in DICOM standard (Rosslyn 1996) in which the patient information including name, birth date, gender, history are included in object classes. This information is sensitive to the patient and important for radiologist diagnosis.

Data security becomes an important issue when brain tumour images are transmitted from examination site to expert center. Figure 1 gives an example of a brain tumour with artificial calcifications inserted. Figure 1a is the original brain tumour, (b) is the brain tumour image with artificial calcifications added, (c) is the magnification of a region containing some added artifacts, and (d) is the subtracted image from original and modified brain tumour. Due to advancement of technology it is easy to do modification in a digital image. For this reason image integrity plays an important role in medical images.

A data hiding technique has the following four basic requirements: imperceptibility, robustness, capacity, and security. Therefore users should develop data hiding according to their application requirement.

Currently data hiding is classified into two groups: spatial domain and frequency domain. Spatial domain technique such as least significant bit method embeds message at least significant bit of an image, vector quantization, patchwork and texture block embeds directly by altering coefficient of an image. A frequency domain technique embeds the message by modulating the coefficients of frequency domain, such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) (Tian 2002).

Figure 1. An example of a brain image with inserted artificial calcifications. (a) The original brain tumour, (b) is the brain tumour image with artificial calcifications added, (c) is the magnification of a region containing some added artifacts, and (d) subtracted image between original and modified image with artifacts.

Trichili *et al* (2002) made a proposal where a virtual border was created to store the watermark in DICOM images. Use of patient data in watermarking is suggested in the works of Acharya *et al* (2003) and Miaou *et al* (2000), hiding data in the LSBs of the image. Reversible watermarking techniques have also been proposed (Zain *et al* 2009), but with a very limited scope. Recent works advocate the use of wavelets to digitally watermark the image (Giakoumaki *et al* 2004; Wakatani 2002). A newer work employs wavelets to introduce multiple watermarking to improve image security (Giakoumaki *et al* 2006). Zhou & Huang (2001) proposed a method to encrypt digital signatures to add integrity and authenticity. Coatrieux & Lecornu (2006) have identified three classes of watermarking algorithms used for medical images. Many papers proposed to embed information in non-ROI region in order not to compromise with diagnoses capabilities (Giakoumaki *et al* 2003, 2005).

2. Methodology

Wavelets are mathematical functions that decompose data into different frequency components and then study each component with a resolution matched to its scale. Wavelets have emerged as powerful new mathematical tools for analysis of complex datasets. The Fourier transform provides representation of an image based only on its frequency content. In discrete cosine transform only spatial correlation of the pixels inside the single 2-D block is considered and the correlation from the pixels of the neighbouring blocks is neglected and does not perform efficiently for binary images characterized by large periods of constant amplitude, followed by brief periods of sharp transitions. Hence this representation is not spatially localized while wavelet functions are localized in space. The Fourier transform decomposes a signal into a spectrum of frequencies whereas the wavelet analysis decomposes a signal into a hierarchy of scales ranging from the coarsest scale.

The DWT is an implementation of the wavelet transform using a discrete set of the wavelet scales and translation obeying some defined rules. For practical computations, it is necessary to discretize the wavelet transform. The scale parameter(s) is (are) discretized on a logarithmic grid. The translation parameter (τ) is then discretized with respect to the scale parameter, i.e., sampling is done on the dyadic (as the base of the logarithm is usually chosen as two) sampling grid. The discretized scale and translation parameters are given by, $s = 2^{-m}$ and $\tau = n2^{-m}$, where $m, n \in \mathbb{Z}$, the set of all integers. Thus, the family of wavelet functions is represented in Eq. (1),

$$\psi_{m,n}(t) = 2^{-m/2} \psi(2^{-m}t - n). \quad (1)$$

The wavelet transform decomposes a signal $x(t)$ into a family of synthesis wavelets as given below in Eqs. (2) and (3),

$$x(t) = \sum_m \sum_n c_{m,n} \psi_{m,n}(t), \quad (2)$$

where

$$c_{m,n} = \langle x(t), \psi_{m,n}(t) \rangle. \quad (3)$$

For a discrete-time signal $x[n]$, the wavelet decomposition on I octaves is given by

$$x[n] = \sum_{i=1 \text{ to } I} \sum_{k \in \mathbb{Z}} c_{i,k} g \left[n - 2^i k \right] + \sum_{k \in \mathbb{Z}} d_{I,k} h_I \left[n - 2^I k \right], \quad (4)$$

where $c_i, k, i = 1 \dots I$: wavelet coefficients and $d_i, k, i = 1 \dots I$: scaling coefficients.

The wavelet and the scaling coefficients are given by

$$c_{i,k} = \sum_n x[n] g_i^*[n - 2^i k], \quad (5)$$

$$d_{i,k} = \sum_n x[n] h_i^*[n - 2^i k], \quad (6)$$

where $g_i[n - 2^i k]$ and $h_i[n - 2^i k]$ represent the discrete wavelets and scaling sequences, respectively, and (*) indicates complex conjugate.

In case of images, the DWT is applied to each dimension separately. This result in an image Y is being decomposed into a first level approximation component Y_a^1 , and detailed components Y_h^1 , Y_v^1 and Y_d^1 ; corresponding to horizontal, vertical and diagonal details (Gonzalez and Woods 2004). Equation (7) depicts the process of an image being decomposed into approximate and detailed components. The approximation component (Y_a) contains low frequency components of the image while the detailed components (Y_h , Y_v and Y_d) contain high frequency components. Thus

$$Y = Y_a^1 + \{Y_h^1 + Y_v^1 + Y_d^1\}. \quad (7)$$

If DWT is applied to Y_a^1 , the second level approximation and detailed components are obtained. Higher-level decomposition is performed similarly. If the process is repeated up to N levels, the image Y can be written in terms of the N^{th} approximation component (Y_a^N) and all the detailed components as given below in Eq. (8),

$$Y = Y_a^N + \sum_{i=1}^N \{Y_h^i + Y_v^i + Y_d^i\}. \quad (8)$$

At each decomposition level, the length of the decomposed signals is half the length of the signal in the previous stage. Hence the size of the approximation component obtained from the first level decomposition of an $N \times N$ image is $N/2 \times N/2$, second level is $N/4 \times N/4$ and third level is $N/8 \times N/8$ and so on. As the level of decomposition is increased, compact but coarser approximation of the image is obtained. Third level of decomposition increases security compared to other levels. Thus, wavelets provide a simple hierarchical framework for interpreting the image information (Koenderink 1984).

The basis of a wavelet transform that is compressed or localized is called the mother wavelet of a wavelet transform. In case of DICOM MRI (Magnetic Resonance Image) or CT (Computer Tomography) images of the brain, can be very effectively represented by a Daubechies-4 (DAUB4) (Daubechies 1992) wavelet though expensive to compute, has the advantage of better resolution for smoothly changing signals compared to Haar wavelet. In this paper, we have applied ROI with DAUB4 wavelet to be embedded in the center of an image.

To meet medical image watermarking security during transmission from examination site to expert center, in our scheme we propose patient id and SOP Instance UID is encrypted using RSA algorithm and embedded in the LSB border of the non-ROI region. Three-level DWT of ROI is embedded in the center of the ROI region as shown in figure 2.

The characteristics of our scheme can be summarized as

- (i) Robust against certain type of attacks such as salt pepper, angle rotation, contrast stretching, shrinking and low pass filter.
- (ii) Reversibility of ROI.

Figure 2. Areas used for embedding watermark.

The following section describes the embedding and extracting procedures.

2.1 Image preprocessing

This includes segmentation of brain tumour and acquiring patient information from the DICOM image header. DICOM image used in our paper is of 512×512 int16 pixels size. The cropping can be done by finding minimum rectangle covering the brain tumour after region based segmentation as shown in figure 3.

2.2 Digital signature

Patient-Id and SOP Instance UID is encrypted using RSA algorithm by obtaining private key from the examination site.

Figure 3. Global region based segmentation.

Figure 4. Watermark embedding steps.

2.3 DWT

ROI image is transformed into 3-level DWT and the wavelet coefficients in LL3 level are represented to 12 bit plane.

2.4 Embedding

The ROI (brain tumour image obtained after region based segmentation and cropping) embedded in the center region of non-ROI of an image as shown in figure 4. The DS is embedded randomly into the border of the image.

2.5 Extraction

Figure 4 shows the decoding procedure for extracting the watermark. The original image stored in database server is required to extract the watermark. If the watermark in the attacked image is failed to extract, the image is re-transmitted to the user. This procedure is reversed as the embedding procedure and it uses the subtraction of watermarked image and the original image as shown in figure 5.

Figure 5. Watermark extraction steps.

3. Results and discussion

DS can be used to verify image authenticity and integrity. Usually DS is attached at the head or at the end of the image data file. In our paper, DS is embedded randomly into the border of the image. Embedding of DS into the border of the image has several advantages. First, it does not change the file size. Second, it does not change the file format. These advantages have add on value because DICOM image format is not changed as per DICOM standard.

Figure 6 depicts the visual aspect of the individual bit planes of brain tumour image shown in figure 1. Individual bit plane demonstrates whether image information is presented at each bit. Bit 1 consists of less useful information, bit 12 consists of maximum information for brain tumour analysis. Original information obtained by accumulating all the 12 bit planes such as 12, 12 + 11, 12 + 11 + 10,.. to obtain original image. First, pixels in a brain tumour image is highly correlated. Second, Least significant bit of an image mostly consists of noise. Although brain tumour is an initialized 16 image, 12 bits of 2 bytes are used, remaining 13, 14, 15, 16 are not used for embedding because some image compression algorithms may clip these bits.

The DS embedded randomly into the border of the LSB image using standard encryption technique RSA. RSA is an effective method for verifying image authenticity and integrity in medical images. The encryption of the text/graphical file and interleaving in the frequency domain using the DCT is suggested in works of Acharya *et al* (2004). Nayak *et al* (2004) proposed DFT was found to be very efficient for Interleaving of the patient information such as text documents and physiological signals with medical images. The wavelet watermarking offers many advantages compared with DFT and DCT watermarking, as shown in (Serdean *et al* 2002).

Watermarking the original image slightly degrades the original images as far as peak signal to noise ratio (PSNR) is concerned. But it is well within the visual perception and we do not readily visualize the watermark and the degradation. The visual quality of the marked image is measured in PSNR.

$$PSNR = 10 \log_{10} \frac{R^2}{MSE}. \quad (9)$$

R the maximum fluctuation in the input image data type.

In addition, a good watermark technique should be robust to withstand different kinds of attacks. In the following experiments, Peak signal to noise ratio (PSNR) of the watermarked image to the original image is about 53 dB (Ni *et al* 2003; Lee *et al* 2004, 2006) and hence quality degradations could hardly be perceived by human eye.

Several common attacks are used to measure the robustness of the proposed scheme, such as salt and pepper noise attack (noise density $d = 0.05$), contrast stretching attack (improve the

Figure 6. Individual bit planes of brain tumour image. From left to right, top to bottom, individual bit plane images of bit 1(LSB),2,3,4,5,6,.....12(MSB).

Table 1. The experimental results of watermarked image under different attacks.

Attack-scheme	PSNR values
Watermarked image	53 dB
Salt and pepper noise attack	24.8052 dB
Contrast stretching attack	24.8088 dB
Shrinking attack	24.7758 dB
Low pass filter attack	24.8088 dB
Angle rotation attack	24.7918 dB

contrast in an image by ‘stretching’ the range of intensity values), shrinking attack (block of row and column is deleted), low pass filter (smoothing) and angle rotation attack ($\theta = 45^\circ$), etc. The detailed experimental results are shown in table 1. We can see that the experimental results are acceptable.

4. Conclusion

In this paper, we proposed a watermarking scheme to enhance medical image and data security. In our scheme least significant bit substitution is adapted to fulfill the requirements of data hiding and authentication in medical images. The scheme divides image into two parts ROI and non-ROI. The DS embedded randomly into the border of the LSB brain image using standard encryption technique. The ROI is embedded in the LSB center of the brain image. Our results demonstrate the effective embedding and retrieval of DS and ROI from the watermarked image, and the results of robustness to different attacks are found to be satisfactory. Currently, investigation is being carried out to enhance the scheme against various attacks.

References

- Acharya U R, Bhat P S, Kumar S, Min L C 2003 Transmission and storage of medical images with patient information. *Comput. Biol. Med.* 33: 303–210
- Acharya U R, Niranjana U C, Iyengar S S, Kannathal N, Lim C M 2004 Simultaneous storage of medical images with patient information. *Comput. Methods Programs Biomed.*, Sweden 76(1): 13–19
- Coatrieux G, Lecornu L 2006 A review of image watermarking applications in healthcare. *Proceedings of the 28th Annual International Conference of the IEEE: Engineering in Medicine and Biology Society, EMBS '06*
- Daubechies I 1992 Ten lectures on wavelets. *CMBS Conference Lecture Notes 61*. SIAM, Philadelphia
- Giakoumaki A, Pavlopoulos S, Koutsouris D 2003 A medical image watermarking scheme based on wavelet transform. *Proceedings of the 25th Annual International Conference of the IEEE EMBS 1*: 856–859
- Giakoumaki A, Pavlopoulos S, Koutsouris D 2004 A multiple watermarking scheme applied to medical image management. *Proc. 26th Annu. Int. Conf. IEEE (EMBS)* 3241–3244
- Giakoumaki A, Pavlopoulos S, Koutsouris D 2005 Multiple digital watermarking applied to medical imaging. *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*
- Giakoumaki A, Pavlopoulos S, Koutsouris D 2006 Secure and efficient health data management through multiple watermarking on medical images. *Med. Biol. Eng. Comput.* 44: 619–631
- Gonzalez R C, Woods R E 2004 *Digital image processing*, 2nd ed., Pearson Education, Ch. Wavelet and Multi Resolution Processing, 349–408

- Koenderink J 1984 The structure of images. *Biol. Cybern.* 50(5): 363–370
- Sang-Kwang Lee, Young-Ho Suh, Yo-Sung Ho 2004 Lossless data hiding based on histogram modification of difference images. *Advances in Multimedia Information Processing*, LNCS 333, 340–347
- Sang-Kwang Lee, Young-Ho Suh, Yo-Sung Ho 2006 *Reversible image authentication based on watermarking*. ICME, IEEE
- Miaou S, Hsu C, Tsai Y, Chao H 2000 A secure data hiding technique with heterogeneous data-combining capability for electronic patient records, presented at the World Congr. Med. Phys. *Biomed. Eng., Proc.*, Session Electron. Healthcare Records (IEEE-BEM), Chicago, IL
- Nayak J, Bhat P S, Acharya U R, Niranjana U C 2004 Simultaneous storage of medical images with patient information: A comparative study. *Biomedical Online Journal, USA* 3: 17. 5th June 2004
- Ni Z, Shi Y, Ansari N, Su W 2003 Reversible data hiding. *Proc. ISCAS* 2: 912–915
- Rosslyn V A 1996 *Digital Imaging and Communications in Medicine (DICOM)*. National Electrical Manufacturers' Association, PS3.1-1996-3
- Serdean C V, Tomlinson M, Wade G J and Ambrose A M 2002 Protecting intellectual rights: digital watermarking in the wavelet domain. *Proceedings of IEEE Intl. Workshop on Trends and Recent Achievements in Information Technology, Cluj-Napoca, Romania* 16–18 May, 70–77
- Tian J 2002 Wavelet based reversible watermarking for authentication. *Proceedings of SPIE on Security and Watermarking of Multimedia Contents IV*, vol. 4675, Jan, 679–690
- Trichili H, Bouhlef M S, Derbel N, Kamoun L 2002 A new medical image watermarking scheme for a better telediagnosis. *Proc. IEEE Int. Conf. Syst., Man Cybern., Session MP1B* 556–559
- Wakatani A 2002 Digital watermarking for ROI medical images by using compressed signature image. *Proc. 35th Hawaii Int. Conf. Syst. Sci.* 2043–2048
- Zain J M, Baldwin L P, Clarke M 2009 Reversible watermarking for authentication of DICOM images. *Proc. 26th Annu. Int. Conf. Eng. Med. Biol. Soc. (EMBC 2004)* 2: 3237–3240
- Zhou X Q, Huang H K 2001 Authenticity and integrity of digital mammography images. *IEEE Trans. Med. Imag.* 20(no. 8): 784–791